RFID 시스템에서의 소유권 이전 프로토콜의 취약성 분석

김동철 천지영 최은영 이동훈
고려대학교 정보경영공학전문대학원*

ifineedu0707@korea.ac.kr, jychun@korea.ac.kr, bluecey@cist.korea.ac.kr,
donghlee@korea.ac.kr

Vulnerability Analysis of Ownership-transfer Protocol in RFID Systems

Dong Cheol Kim, Ji Young Chun, Eun Young Choi, Dong Hoon Lee
Graduate School of Information Management and Security, Korea University

요약

최근 사물에 태그를 부착하여 사물의 정보를 확인하고 주변의 상황을 감지하는 RFID(Radio Frequency Identification)시스템이 등장하여 유비쿼터스 사회의 기반 기술 중 하나로 주목받고 있다. 하지만 현재 RFID 관련 산업들은 개인 프라이버시 침해 문제로 실생활 적용에 많은 어려움을 겪고 있다. 이에 정부 및 여러 연구기관에서는 RFID 시스템에서의 개인 프라이버시를 보호하기 위한 연구가 활발하게 진행 중이다. 하지만 이러한 연구들은 태그와 리더사이 무선공간에서의 도청 등을 통한 정보유출 및 위치추적 등의 문제를 다루고는 있지만, 소유권 이전 발생 시 프라이버시를 보호하는 문제는 다루지 않고 있다. 태그가 부착된 사물들 중에는 개인소유의 물품들이 존재하며, 이 사물들은 한 사람에게 평생 소유될 수도 있지만, 다른 사람에게 소유권을 이전해야 하는 경우가 발생한다. 하지만 현재 RFID 시스템에서는 이에 대한 기술 및 연구가 부족하다. 따라서 본 논문에서는 RFID 시스템에서의 소유권이전 문제에 대한 중요성을 기술하고 현재까지 제안된 RFID 시스템에서의 안전하게 소유권을 이전 할 수 있는 기법들을 알아본다. 그리고 제안된 기법들의 취약성을 분석하여 앞으로의 연구방향을 제시한다.

1. 서론

최근 사물에 태그를 부착하여 사물의 정보를 확인하고 주변 상황을 감지하는 RFID(Radio Frequency Identification)시스템이 등장하여 유비쿼터스 사회의 기반 기술 중 하나로 주목받고 있다. RFID 시스템이란 마이크로 칩을 내장한 태그에 저장된 데이터를 무선 주파수를 이용하여 객체 식별 장비인 리더기를 통해 자동 인식되는 기술을 말한다. 이러한 기술은 칩의 저장능력과 비접촉식 무선통신으로 인해 기존의 바코드를 대체할 기술로 주목받고 있다. 하지만 이러한 RFID 시스템은 도청, 트래픽분석 등 여러 방법을 통해 누구든지 태그에 내장된 물품에 대한 정보를 쉽게 얻을 수 있고, ID의 유일성을 이용해 태그 사용자의 위치추적을 가능하게 함으로서 사용자의 프라이버시가 쉽게 노출되는 문제를 지니고 있다. 이에 정부 및 여러 연구기관에서는 RFID 시스템에서의 개인 프라이버시를 보호하기 위한 연구가 활발하게 진행 중[1,4,5]이다.

하지만 이러한 연구들은 태그와 리더 간 무선공간에서의 도청 등을 통한 정보유출 및 위치추적 등의 문제를 다루고는 있지만, RFID 태그가 부착된 사물에 대한 소유권 이전 발생 시 프라이버시를 보호하는 문제는 다루지 않고 있다. 태그가 부착된 사물들 중에는 개인소유의 물품들이 존재하며, 이 사물들은 한 사람에게 평생 소유될 수도 있지만, 다른 사람에게 소유권을 이전해야 하는 경우가 발생한다. 하지만 현 RFID 시스템에서는 이에 대한 기술적 지원 부족으로 개인의 프라이버시 침해가 발생한다. 다시 말하면, 이전 소유자는 이전한 물품들에 대한 접근이 제한되어야 하지만 이전 소유자는 소유권 이전 이후에도 여전히 이전한 사물들에 접근이 가능하다. 이를 통해 이전 소유자는 언제든지 이전한 물품을 소유한 사람의 위치추적이 가능하며, 현 소유자의 프라이버시를 침해할 수도 있다. 이것은 앞으로 모든 사물에 RFID 태그를 부착하고자 하는 RFID 산업에 큰 문제이다. 따라서 우리는 본 논문에서 현재까지 제안된

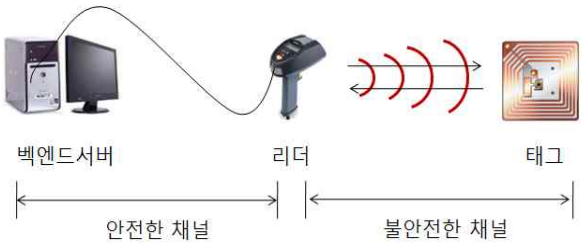
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

RFID 시스템에서의 안전한 소유권 이전 기법들을 알아보고 분석하여 문제점을 지적한다. 그리고 앞으로의 연구방향을 제시한다.

본 논문의 구성은 2장에서 간단히 RFID 시스템에 대한 간단한 설명하고 3장에서는 현재까지 제안된 RFID 시스템에서의 소유권 이전 프로토콜을 기술한다. 4장에서는 제안된 기법들의 취약성을 분석하고 5장에서는 결론과 함께 앞으로의 연구방향을 제시한다.

2. RFID 시스템의 구성

RFID 시스템은 태그, 리더, 벡엔드 서버의 세가지 요소로 구성 되어 있다.



[그림 1] RFID 시스템 구성도

1) 태그 : 일반적으로 IC칩과 안테나(antenna)로 구성되어 있다. 리더가 질의(query)를 보내면, 내부에 가지고 있는 정보나 그 정보를 가지고 계산한 결과 값을 리더에게 송신해 주는 것이 태그의 일반적인 역할이다. 태그는 크게 능동형 태그와 수동형 태그로 분류될 수 있다.
2) 리더 : 태그에게 요청신호를 보내고 태그로부터 정보를 받은 후, 벡엔드 서버시스템으로 정보를 보내거나 벡엔드 시스템으로부터 정보를 받아 태그에 쓰기를 하는 역할을 한다.
3) 벡엔드 서버 : 다수의 리더로부터 전송되어 오는 태그 관련 정보에 대한 처리를 해주는 서버 시스템이다. 벡엔드 서버는 보안 측면에서 신뢰할 수 있는 시스템으로 간주된다.

태그-리더간 통신은 무선통신이기 때문에 도청이 가능하지만, 리더-벡엔드 서버간의 통신은 안전한 채널을 통해서 이루어진다고 가정한다.

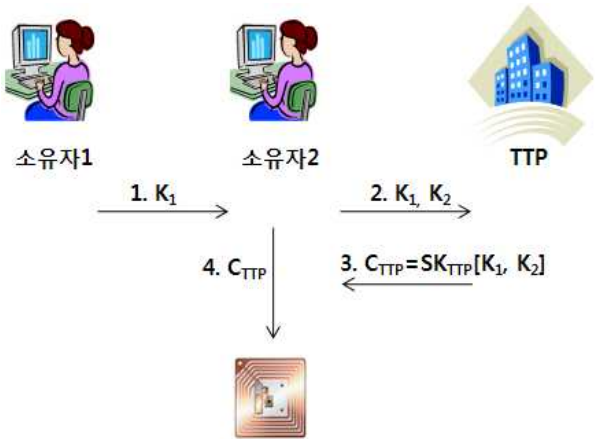
3. 소유권 이전 프로토콜

현재까지 제안된 RFID 시스템에서의 안전하게 소유권을 이전하기 위한 프로토콜은 많지 않다. 본 논문에서는 RFID 시스템에서의 소유권이전을 처음으로 제안한 Junichiro Saito et al 기법과 최근에 Kyosuke Osaka et al 이 제안한 기법을 기술한다.

3.1 J. Saito et al's 기법

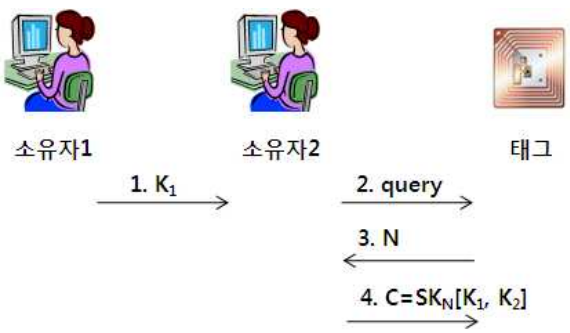
제안된 기법[2]은 대칭키를 사용한 기법으로 RFID 태그의 ID 정보를 대칭키를 사용하여 암호화한다. 따라서 이전 소유자는 암호화 키를 새로운 소유자에게 전달하고 새로운 소유자는 그 키를 새로운 키로 바꾼다. 결국 이전 소유자는 ID정보를 복호화 할 수 없게 된다. 제안된 기법은 TTP를 이용한 기법과 이용하지 않은 기법으로 두가지로 나뉜다.

1) TTP를 포함한 소유권 이전 프로토콜
   a) 소유자1 → 소유자2 : 대칭키 k_1을 전송
   b) 소유자2 → TTP : k_1, k_2(새로운 대칭키) 전송
   c) TTP → 소유자2 : $C_{TTP}=SK_{TTP}[k_1,k_2]$를 전송
   d) 소유자2 → 태그 : C_{TTP}
   e) 태그 : C_{TTP}를 복호화, k_1의 확인 및 k_2 업데이트



[그림 2] TTP를 포함한 소유권 이전 프로토콜

2) TTP없는 소유권 이전 프로토콜
   a) 소유자1 → 소유자2 : 대칭키 k_1을 전송
   b) 소유자2 → 태그 : 요청메세지(query) 전송
   c) 태그 → 소유자2 : 난수 N 전송
   d) 소유자2 → 태그 : $C=SK_N[k_1,k_2]$ 전송
   e) 태그 : C 복호화, k_1 확인 및 k_2 업데이트



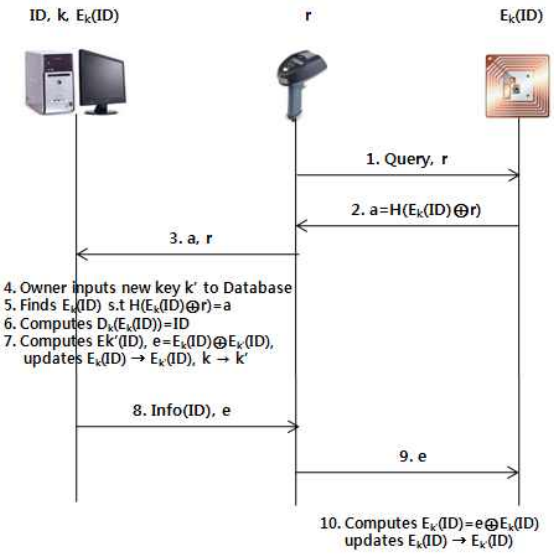
[그림 3] TTP없는 소유권 이전 프로토콜

3.2 K. Osaka et al's 기법

제안된 기법[3]은 해쉬함수와 대칭키 암호시스템을 기반으로한 기법으로 다음의 세가지 과정으로 이루어져 있다. 쓰기과정(Writing process), 인증과정(authentication process), 소유권이전과정(Ownership transfer process)

가. 쓰기 과정

태그 제조자는 대칭키 k를 생성한 후 $E_k(ID)$를 생성하고 태그에 쓴다. (제조자 리더 → 태그 : $E_k(ID)$)



[그림 4] 인증과정

나. 인증 과정

1) 리더는 요청신호(query)와 랜덤값 r을 태그에게 전송한다.

2) 태그는 $a=(H(E_k(ID)\oplus r)$을 계산하고 리더에게 전송한다. 그리고 리더는 a, r을 벡엔드 서버에 전송한다.

3) 벡엔드 서버는 리더로부터 온 a값을 이용하여 $E_k(ID)$를 찾기 시도한다. 그러면 벡엔드 서버는 $D_k(E_k(ID))$를 통해 ID값을 얻어 낼 수 있다. 그래서 벡엔드 서버는 Info(ID)값을 리더에게 전송한다. 이 때 만약에 소유권 이전이 필요없다면 인증과정을 종료한다. 하지만 만약에 소유권 이전이 필요한 상황이라면 다음의 소유권이전 과정을 거친다.

4) 소유자는 새로운 대칭키 k′를 벡엔드 서버에 보낸다. 벡엔드 서버는 ID를 새로운 대칭키로 암호화한다. 그러면 벡엔드 서버는 $e=E_k(ID)\oplus E_{k'}(ID)$를 계산한다. 그리고 데이터베이스는 k를 k′으로 $E_k(ID)$를 $E_{k'}(ID)$로 업데이트 한다. 마지막으로 벡엔드 서버는 Info(ID)와 e를 리더에게 전송하고, 리더는 Info(ID)와 e를 태그에게 전송한다.

5) 태그는 e로부터 $E_{k'}(ID)$를 계산하고 $E_k(ID)$를 $E_{k'}(ID)$로 업데이트 한다.

다. 소유권이전 과정

1) 현재 소유자는 현재의 대칭키 k를 새로운 대칭키 k′으로 바꾼다. 그리고 안전한 채널을 통해 (k′, ID, Info(ID), etc.)를 새로운 소유자에게 전달한다.

2) 새로운 소유자는 받은 대칭키 k‘을 또 새로운 k′′로 바꾸고 새로운 소유자는 k′′를 자신의 새로운 대칭키로 사용한다.

4. 제안된 기법들의 취약성

위에 제안된 기법들은 각각 다음과 같은 취약성을 지니고 있다.

4.1 J. Saito et al's 기법의 취약성

1) TTP를 포함한 소유권 이전 프로토콜에서 TTP와 태그는 항상 공유된 대칭키를 보유한다. 만약 모든 태그들이 유일한 각각의 대칭키를 보유한다면, TTP는 수십, 수백만개가 넘는 태그의 키를 관리해야 하기 때문에 매우 비효율적이다.

2) 태그는 TTP와 대칭키를 보유하는데, 태그 소유자는 그 공유키를 알아낼 수 있다. 따라서 소유권 이전 이후에 태그에 접근할 수 있어 심각한 프라이버시 침해가 발생할 수 있다.

3) TTP가 없는 소유권이전 프로토콜에서의 이전 사용자는 벡워드 채널에서 태그로부터 전송되는 난수를 도청하여 자신이 가졌던 대칭키 k1을 이용하여 k_2의 값을 알아낼 수 있다. 이전 이후에도 태그를 접근제어 할 수 있다.

4) 두 프로토콜 모두 소유권이전 발생 시 태그를 인증하는 과정이 빠져 있기 때문에, 이전소유자 또는 공격자는 복제된 태그 또는 가짜 태그를 만들어 소유권을 양도 받은 소유자를 속일 수 있다.

4.2 K. Osaka et al's 기법 취약성

1) 마지막 리더가 태그에게 e값을 전송할 때 공격자가 전송값을 가로채거나 바꾼다면 태그와 벡엔드 서버사이에는 동기화가 깨지게 된다. 따라서 이 후 프로토콜을 수행 할 수 없다.

2) 인증과정 중 태그는 따로 난수값을 생성하지 않기 때문에 첫 번째 요청신호를 보낼 때 같이 보내는 난수를 공격자가 가로채어 자신이 생성한 값을 태그에 전송한다면 태그는 항상 일정한 값을 내놓기 때문에 위치추적이 가능하게 된다.

5. 결론

지금까지 RFID 시스템에서 제안된 소유권 이전 프로토콜을 알아 보았다. 하지만 제안된 기법들은 위에서 언급한 것과 같이 아직 많은 취약성을 가지고 있어 프라이버시를 보호해야 하는 RFID 시스템에 적용하기에는 어려움이 있다. RFID시스템에서의 안전한 소유권 이전은 이전소유자로부터 현재 소유자의 프라이버시를 보호하는 것이다. 앞으로 모든 사물에는 RFID 태그가 부착될 것으로 예상되며

가장 먼저 선결되어야 하는 것 중에 하나가 프라이버시 보호이다. 따라서 우리는 프라이버시를 보호하기 위한 연구에 소유권 이전시 발생할 수 있는 문제에 대해서도 인지하고 이 분야에 관련된 연구가 활발하게 이루어져야 할 것이다.

참고문헌

[1] Dirk Henrici and Paul Muller "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers" Workshop on Pervasive Computing and Communications Security (PerSec'04) at IEEE PerCom 2004l. March 14-17, 2004

[2] J. Saito, K. Imamoto, K. Sakurai, "Reassignment Scheme of an RFID Tag's Key for Owner Transfer", Embedded and Ubiquitous Computing - EUC2005 Workshops. LNCS, vol. 3823, pp.1303-1312

[3] K. Osaka, T. Takagi, K. Yamazaki, O. Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer", computational Intelligence and Security, volume 2, 2006, pp. 1090-1

[4] M. Ohkubo. K, Suxuki and S. Kinoshita "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubcomp2004 workshop.

[5] Weis, Stephen and Sarma, Sanjay and Rivest, Ronald and Engels, Daniel "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems" International Conference on Security in Pervasive Computing. SPC 2003.3